Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matters of	)	
	)	
A National Broadband Plan for Our Future	)	GN Docket No. 09-51
	)	
International Comparison and Consumer Survey Requirements in the Broadband Data Improvement Act	)	GN Docket No. 09-47
	)	
Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act	)	GN Docket No. 09-137

COMMENTS-NBP PUBLIC NOTICE #8
OF QWEST COMMUNICATIONS INTERNATIONAL INC.

Craig J. Brown
Lawrence E. Sarjeant
Suite 950
607 14th Street, N.W.
Washington, DC 20005
(202) 429-3112
Craig.Brown@qwest.com
Lawrence.Sarjeant@qwest.com

Attorneys for

QWEST COMMUNICATIONS
INTERNATIONAL INC.

November 12, 2009

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matters of	)	
	)	
A National Broadband Plan for Our Future	)	GN Docket No. 09-51
	)	
International Comparison and Consumer Survey Requirements in the Broadband Data Improvement Act	)	GN Docket No. 09-47
	)	
Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act	)	GN Docket No. 09-137

COMMENTS-NBP PUBLIC NOTICE #8
OF QWEST COMMUNICATIONS INTERNATIONAL INC.

In these comments, Qwest Communications International Inc. (Qwest) responds to questions concerning Next Generation 911 (NG911) and cyber security presented in NBP Public Notice #8, issued by the Commission in the above-referenced proceedings on September 28, 2009.[1]

I. INTRODUCTION AND SUMMARY

Today's 911 and E911 systems were not deployed with the intention that they would process voice and data communications from IP-enabled devices. Consideration of standards and best practices is underway that will facilitate the full convergence of circuit switched and data networks into a NG911 design using IP-capable emergency communications networks.

---

[1] Public Notice, DA 09-2133, *Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan*, NBP Public Notice #8, rel. Sept. 28, 2009.

Although important work is underway, completion of the migration to a national NG911 network capable of sending and receiving interactive data and video content in IP format is still in the future.

Transitional steps are required to accommodate the co-existence of interconnected circuit switched and next generation networks that mutually and reliably support, at a minimum, the emergency response services that the Nation has come to depend upon. There are many aspects to a successful and complete transition. Among them are the development of regulatory[2] and technical standards, best practices, and efficient governance processes. Significant infrastructure investments[3] will be required in order to ensure continuity during the transition and to complete the conversion to a national NG911 network that is accessible anytime, anywhere, from any device. Another significant factor for the successful migration to a national NG911 network is adequate PSAP funding to permit universal PSAP acquisition and implementation of NG911 solutions.

Qwest is constantly evaluating new technologies that can enhance its customers' communications experience, including those related to NG911 service. The ongoing process of seeking to perfect the customer's experience demands that Qwest weigh the benefits and costs that any particular technology or solution produces for its customers. Accomplishing the conversion to NG911 will substantially enhance the capabilities of emergency responders and thereby improve public safety generally for the Nation. All stakeholders in this effort must be

---

[2] Clarity as to the jurisdictional authority to be exercised by federal and state regulatory bodies is essential to avoid duplicative or conflicting requirements and practices, which would serve to slow the NG911 transition and increase its cost.

[3] The infrastructure required will not necessarily be 911-specific as NG911 will largely be software driven.

unified in their resolve to work cooperatively to identify and implement the most cost-effective solutions for the migration and ultimate conversion to a national NG911 network.

As a network services provider, Qwest has long supported the ongoing federal government focus on cyber security. Qwest has worked through the primary public-private venues to actively address evolving issues associated with protecting its networks and the information that flows across those networks. Like its peers, Qwest works diligently every day with the government and other private sector entities to thwart all types of cyber attacks that come from all corners of the globe. Qwest employs widely accepted best practices in order to maintain a vigilant, proactive cyber security posture. The use of voluntary best practices has proven to be an effective means to facilitate the implementation of protective measures and effectively manage risk. To the extent that further refinement of existing carrier/ISP practices is needed in order to respond to evolving cyber threats, Qwest believes the focus should be on voluntary best practices developed collaboratively by the private sector and government.

Qwest also supports customer education on cyber security issues. Qwest's efforts include its online Incredible Internet site (www.incredibleinternet.com), which provides information regarding online safety, cyber bullying, identity theft, as well as a free Internet safety on-line help desk and a hot line provided by the National Center for Missing and Exploited Children.

II. DISCUSSION

A. Next Generation 911

1. The Broadband Infrastructure Requirements for NG911

Qwest's experiences with 911, E911 and the work being done associated with the migration to a NG911 network lead it to conclude that facilitation of an efficient and cost-effective migration process will be as important in achieving a successful conversion as having a clear understanding of the infrastructure requirements for the NG911 network. The process of

migrating to a NG911 network cannot be defined as a single event or solution. Rather, the migration will proceed through various iterations that will be driven, in part, by the numerous and varied priorities that exist within the PSAP community. Qwest sees three distinct aspects of the migration associated with infrastructure requirements. First, an overlay IP transport network that will enable PSAPs to receive TDM or IP originated 911 calls in IP format must be deployed. Second, there must be a replacement of PSAPs' existing TDM equipment with IP capable equipment. Third, applications that will enable emergency service providers, including PSAPs, to perform enhanced functions[4] must be secured and deployed.[5]

The essential building blocks for NG911 are: the establishment of an IP-based transport network from individual PSAPs to selective routers that is capable of providing the additional bandwidth necessary to support the delivery of voice and data to the PSAPs; and the acquisition and deployment of the IP-capable equipment needed to manage the flow and distribution of the traffic. Today, that transport is provided for 911/E911 calls over very low capacity voice grade circuits that are not capable of accommodating the higher bandwidth requirements of IP traffic. Qwest sees the necessary migration strategy as non-linear. It envisions installing an IP private port and local loop as a replacement for the existing analog point-to-point network at a number of different locations in its network. Further, it is anticipated that the IP configuration will be supported with gateways at either the ingress or egress points, or both. This will allow 911 calls in the next generation environment to originate and terminate using alternative protocols such as IP or TDM/analog (or in the case of ALI, IP or ASCII).

---

[4] *E.g.*, responding to text messages and video applications and providing critical medical information to emergency responders at an accident or crime scene.

[5] Some PSAPs are securing transport capability now in anticipation of the availability of desired applications at a later date. Other PSAPs are working through local issues, such as funding, and may secure transport capability when the desired applications become available.

Qwest has introduced a data complex. At its core, the data complex is analogous to an IP selective router. Predicated on the same philosophy of needing to receive and distribute voice and data using alternative protocols, the data complex is more than a selective router. It is within the data complex that feature functionality such as ALI steering or Geospatial MSAGing will be performed using current standards. The data complex is also integral to the IP-based infrastructure that will support future standards-based features and functions such as the receipt and distribution of text messages and streaming video.

Full conversion to a NG911 network requires PSAP upgrades of network facilities and equipment at their premises to enable their receipt of 911 communications in an IP format. While there is much to be done on the part of network services providers to deploy NG911 capable network facilities, it is important for the Commission to appreciate that some necessary network elements associated with the NG911 network are owned or controlled by PSAPs. Their ability to make the needed upgrades in their networks directly bears on when the conversion to NG911 can be completed.

The third aspect of the NG911 migration is the introduction of yet to be developed applications that will be broadly available to public safety officials for use when they respond to emergency situations. Such applications could include: text location detection and selective routing; human and non-human video applications; inclusion of automatic crash notification supplementary data; disparate GIS integration; vital health supplemental data; time of day routing; and incident management. In response to specific PSAP requests, Qwest has introduced an IP solution set that allows PSAPs to begin migrating from the legacy network at a pace and in a sequence that meets their needs.

2. The Scope of NG911 Technology and Service Deployment Today

Qwest has received and responded to several state-wide NG911 requests for proposals representing approximately one third of the PSAPs supported by Qwest. The requirements contained in the customers' RFPs typically leverage existing standards. Those requirements are primarily driven by the customers' recognition that greater bandwidth in the 911 infrastructure is necessary in order to support enhanced emergency services capabilities such as text and video. Some states are prepared to award contracts for:

> iQ MPLS Private Port with local loop and integrated management to replace the EM trunks between the legacy selective router and the PSAP;
>
> ingress gateways and routers to receive TDM/analog-based calls from the E911selective router;[6]
>
> Emergency Call Management Complex (ECMC);[7] and
>
> PSAP Gateway modules.[8]

B. Cyber Security

1. Responses to Computer-based Attacks Against Government or Commercial Computer Systems or Networks

Computer-based attacks against computer systems and networks frequently involve malicious software such as viruses, trojans, worms, and botnets;[9] e-mail threats that include

---

[6] The purpose of these gateways is to manage the protocol conversion required to place the caller's voice and Automatic Number Identification (ANI) onto a Qwest provided MPLS private port network for delivery to an IP-based selective router. Telecommunications Services Providers (TSPs) will retain their connection to the current routers. At some point in the future, based on the PSAPs' requirements, the TSPs will be given the opportunity to connect directly to the ingress gateways and bypass the legacy routers.

[7] The ECMC will manage the call routing and default routing functions on the IP network, replicating the primary functions of the legacy selective routers. As the systems evolve, the ECMC will provide the ingress and management functions for the emerging methods for requesting emergency response.

[8] These devices will be placed at the PSAP and will convert the IP call back to a TDM/analog format until the PSAP ANI/ALI controller can receive the call in an IP format.

SPAM and phishing schemes; and denial of service attacks directed at computing or network infrastructures. Commercial carriers constantly invest in new technologies, processes, and people to prevent, detect and respond to cyber attacks. Qwest defends against cyber attacks by:

> Dropping spoofed packets;
> restricting Internet services to subscribers;
> hardening, testing and patching servers and network elements;
> authenticating and filtering Internet protocols;
> limiting the amount of email each customer can send to prevent spam;
> scanning and cleaning malicious software (malware) in email; and
> employing many other techniques.

Qwest has been proactively notifying customers of malware infections for nearly ten years. Qwest developed one of the first automated malware notification and remediation systems for residential customers in 2005.[10] Qwest has proactively notified over one hundred thousand customers using the system. Security software is provided at no additional charge for residential and small office/home office broadband customers to defend against computer malware infections. In addition, customers are provided with printed and electronic information on how to protect their computers, secure wireless access points, the importance of keeping their operating systems and applications patched, and installing and keeping anti-virus software and firewalls updated.

Qwest monitors cyber attacks by observing netflow,[11] the domain name system, email and other Internet service trends and loads. It identifies unusual traffic and server and network

---

[9] Virus - A program or segment of code that is loaded onto a computer without the user's knowledge and runs without the user's consent. Trojan - A harmful program disguised as a harmless application. Worm - A typically harmful program that replicates itself over a computer network. Botnet - A collection of software robots, or "bots," that operate automatically and independently.

[10] *See* Oct. 2, 2007, Press Release discussing it at http://news.qwest.com/index.php?s=43&item=305.

[11] The flow and volume of packet traffic.

element loads. It employs customer and trusted third party notifications, Intrusion Detection Service monitoring and other techniques. Responses to cyber attacks vary greatly depending on the nature of the attack, the harm caused by the attack, and the severity of the attack. Qwest and other carriers have developed an extensive set of tools to mitigate the harm caused by cyber attacks against their networks. Qwest has mature processes and procedures in place and experienced staff that are activated in response to cyber attacks.

2. The Communications Sector is Collaborating with Federal Agencies and Other Governments to Prevent, Detect, and Respond to Cyber Attacks

For 25 years, Qwest has collaborated with the Department of Defense (DoD), and more recently the Department of Homeland Security (DHS), to protect communication sector assets. Historically, this collaboration focused on protecting communication sector assets from physical threats. Current efforts focus on programs to prevent, detect and respond to physical and cyber threats. DHS sponsors public-private organizations that facilitate coordination of the communications sector's policy development, planning and operational activities with the federal government. Policy issues are generally addressed through the President's National Security Telecommunications Advisory Committee (NSTAC). Planning activities are coordinated with DHS through the Communications Sector Coordinating Council (CSCC), and operational activities are conducted through the National Coordinating Center (NCC) within DHS. Qwest is an active member of all three organizations and recently participated in President Obama's Cyberspace Policy Review[12] and DHS's national Cyber Storm exercise.[13]

---

[12] A sixty-day, interagency cyber space policy review led by Melissa Hathaway, then Acting Senior Director for Cyberspace for the National Security and Homeland Security Councils, was completed in mid-April 2009, and the results were made public on May 29, 2009. *See Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.*

While the US Computer Emergency Response Team (US-CERT), DoD and NCC communication sector members interact on a regular basis to address cyber events such as Conficker[14] and denial of service attacks targeting government agencies, the opportunity exists to further improve cyber collaboration efforts with the federal government. Currently, attention is focused on developing a capability within DHS to share actionable cyber information with the private sector as well as a protocol to better coordinate cyber responses within the government and between the government and the private sector. On October 30, 2009, DHS took the first of three steps and co-located the NCC and the US-CERT on one common watch floor called the National Cybersecurity & Communications Integration Center (NCCIC). In subsequent phases, DHS will add even more private sector partners and government participants which should enhance physical and cyber situational awareness and responsiveness to cyber threats. This should also enable better cyber attack defense and coordination.

The NSTAC created the Network Security Information Exchange (NSIE). NSIE representatives include subject matter experts from the government and the private sector that are engaged in the prevention, detection, and/or investigation of telecommunication software penetrations or have security and investigative responsibilities. These experts voluntarily share sensitive information on threats to the operations, administration, maintenance and provisioning systems that support the telecommunications infrastructure.

---

[13] Cyber Storm is the Department of Homeland Security's biennial exercise series. It provides the framework for the most extensive government-sponsored cyber security exercise of its kind. Congress mandated the Cyber Storm exercise series to strengthen cyber preparedness in the public and private sectors. Securing cyber space is the National Cybersecurity Division's (NCSD) top priority. DHS's NCSD works collaboratively with public, private and international entities to secure cyberspace and America's cyber assets.

[14] "Conficker, also known as Downup, Downandup, Conflicker, and Kido, is a computer worm that surfaced November 21st, 2008 with Conficker.A and targets the Microsoft Windows operating system." http://confickerworkinggroup.org/wiki/.

Qwest is also a member of DHS's Cross Sector Cyber Security Working Group (CSCSWG). The CSCSWG was established to address cross sector cyber risks and interdependencies. The CSCSWG engages with DHS and other federal agencies. It provides guidance on government incentives to improve the private sector's cyber security posture and develops metrics to assess cyber security across the 18 critical infrastructure sectors. The CSCSWG is participating in the development of the National Cyber Incident Response Plan.

As an NCC industry member, Qwest provides input to international government organizations such as the US/Canada Civil Emergency Planning Telecommunications Advisory Group (CEPTAG), the North Atlantic Treaty Organization's Civil Communications Planning Committee (NATO CCPC), the US/United Kingdom Joint Contact Group, and the International Telecommunications Union (ITU). These international organizations support government and private industry collaboration to enhance the cyber security posture of computing and network infrastructures globally.

3. Commercial Communications Network Providers Have Incentives to Invest in Secure Infrastructure

Network services providers have strong incentives to maintain secure networks. For example, customer malware infections drive a wide range of additional costs for network services providers. As a result, network services providers have begun implementing programs to reduce malware infections among their customers. Customer service level agreements that impose penalties against network services providers when service levels are impacted by cyber events, and generally high customer reliability expectations, provide additional incentives to maintain secure networks.

4. Cyber Security Best Practices Are Being Employed by Communications Network Providers

Network services providers have heavily invested in cyber security by employing both formal and informal best practices. Cyber security best practices include a host of measures that can be found in many locations. The following is an illustrative list of these locations: Internet Engineering Task Force Standards and Best Current Practice documents; National Reliability and Interoperability Council cyber security best practices; National Institute of Standards and Technology publications; ITU recommendations; International Organization for Standardizations standards; and Alliance for Telecommunications Industry Solutions standards.

III. CONCLUSION

Important work to facilitate the migration to a national NG911 network is underway, but a complete conversion is in the future. Tasks remaining to be completed include the development of regulatory and technical standards, best practices and efficient governance processes. Securing sufficient funding for PSAPs' acquisition and implementation of NG911 solutions continues to be an important factor in moving the migration forward. Qwest has worked cooperatively with PSAPs, introduced a data complex and responded to state-wide NG911 RFPs. Still, additional upgrades in PSAP networks and the acquisition by PSAPs of new applications that will provide enhanced capabilities are integral elements for actualizing the envisioned emergency communications network of the future.

Commercial communications network services providers have been responding to physical and cyber threats to their networks for years. Responses to cyber attacks have varied depending upon the nature of the attack, the harms caused and their severity. Service providers such as Qwest have developed an extensive set of proactive and responsive tools to confront and mitigate the harms to their networks and their customers caused by cyber attacks.

Qwest has collaborated with government entities for 25 years to protect communications sector assets. The public-private collaborative approach to addressing threats to the communications infrastructure has served the Nation well. Qwest believes that there is an opportunity to improve upon the successes of the past as government and industry confront present and future cyber threats. Increased information sharing by government with the private sector would improve overall physical and cyber situational awareness and thereby enhance responsiveness to cyber threats. Qwest fully supports the development of such information sharing capabilities.

Qwest and its peers have strong incentives to maintain secure networks. Qwest currently employs broadly accepted best practices to defend against cyber threats. Qwest believes that the employment of voluntary best practices by network services providers continues to be the most efficacious approach to maintaining a vigilant, proactive cyber security posture. Additionally, Qwest supports customer education on cyber security issues.

Respectfully submitted,

QWEST COMMUNICATIONS
INTERNATIONAL INC.

By: /s/Lawrence E. Sarjeant

Craig J. Brown
Lawrence E. Sarjeant
Suite 950
607 14th Street, N.W.
Washington, DC 20005
(202) 429-3112
Craig.Brown@qwest.com
Lawrence.Sarjeant@qwest.com

November 12, 2009

Its Attorneys

CERTIFICATE OF SERVICE

I, Richard Grozier, do hereby certify that I have caused the foregoing **COMMENTS-NBP PUBLIC NOTICE #8 OF QWEST COMMUNICATIONS INTERNATIONAL INC.** to be: 1) filed with the FCC via its Electronic Comment Filing System in GN Docket Nos. 09-51, 09-47 and 09-137; and 2) served via e-mail on the FCC's duplicating contractor, Best Copy and Printing, Inc. at fcc@bcpiweb.com.

/s/Richard Grozier

November 12, 2009